

JUSTIFICATION FOR OTHER THAN FULL AND OPEN COMPETITION

1. Contracting Activity: Department of Veterans Affairs
Office of Acquisition and Logistics
Technology Acquisition Center
23 Christopher Way
Eatontown, NJ 07724
2. Description of Action: The proposed action is to place a firm-fixed-price delivery order to be issued under the terms and conditions of the National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) V Governmentwide Acquisition Contract (GWAC) for brand name FireEye, Inc. (FireEye) malware protection security appliances, software licenses, warranty and maintenance support.
3. Description of the Supplies or Services: The proposed action is to acquire one brand name FireEye malware protection security appliances, with associated software licenses, warranty and maintenance support for the Office of Information and Technology, Service Delivery and Engineering, Enterprise Operations (EO). EO has a requirement to expand its existing FireEye architecture and infrastructure with an additional malware protection appliance, central management appliance and forensic data analysis appliance to provide enhanced network monitoring capabilities. EO also requires warranty and maintenance support for the additional FireEye appliances. The required warranty and maintenance support includes 24/7 telephone and web support, firmware updates, software updates, patches, and defect support for a period of one year. The period of performance for delivery of malware protection security appliances and associated software shall be 30 days after contract award. Warranty and maintenance support shall be provided for 12-months following acceptance of the appliances.
4. Statutory Authority: The statutory authority permitting an exception to fair opportunity is Section 41 U.S.C. 4106(c)(2) as implemented by the Federal Acquisition Regulation (FAR) Subpart 16.505(b)(2)(i)(B), entitled "Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized."
5. Rationale Supporting Use of Authority Cited Above: Based on the market research described in section eight of this document, it has been determined that limited competition is viable among authorized resellers of the required brand name FireEye appliances, software licenses, and associated warranty and maintenance support. The existing EO network monitoring architecture and infrastructure utilizes only existing FireEye malware protection appliances located at five EO data centers, and EO requires additional appliances that are interoperable and compatible with the existing infrastructure. No other malware protection appliances are interoperable or compatible with the existing FireEye-based malware protection security appliances and architecture. Specifically, the current appliances and associated software communicates through a proprietary source code, and no other software can provide communication capabilities with other malware protection appliances without this

proprietary source code. Further, FireEye is the only security appliance that can provide upstream forwarding of any localized malware activity data within the existing FireEye architecture. The upstream forwarding of malware data produces a single collective status view of all security-related activity over the network and displays the security posture of all assets operating on the network. No other brand name hardware and software appliance can provide this VA required functionality, because no other product can communicate or integrate with the existing FireEye architecture, infrastructure, and software with the existing single collective view EO Console, and thus will not allow for monitoring and visibility of malware activity on the network.

While other devices, identified in section eight of this document, can provide malware protection and monitoring, no other products are interoperable with EO's existing FireEye architecture and infrastructure. Therefore, no other product can operate in VA's FireEye architecture and infrastructure. Additionally, data monitoring and malware activity captured by another product will not integrate with the existing EO FireEye infrastructure components. Acquisition of different network monitoring devices and support would require a completely separate infrastructure to support a new malware protection appliance, resulting in duplication of costs previously expended in acquiring the existing infrastructure that would not be recovered through competition.

Additionally, the required software licenses, warranty and maintenance support, which consists of proprietary software updates, firmware updates, patches, and defect support can only be provided by FireEye or an authorized reseller. The proprietary source code is not available to third-party vendors; therefore, no other vendor other than FireEye or its authorized resellers are capable of providing the required software and firmware updates for FireEye products.

6. Efforts to Obtain Competition: Market research was conducted, details of which are in section eight of this document. Although the Government is limiting competition as a result of specifying a brand name, there are multiple authorized resellers of brand name FireEye hardware, software, and associated warranty and maintenance support on the NASA SEWP V GWAC. This justification will be posted along with the solicitation in accordance with FAR 16.505(a)(4)(iii)(A). Furthermore, in accordance with FAR 5.301 and 16.505(b)(2)(ii)(D), this action will be synopsisized at award on the Federal Business Opportunities Page and the justification will be made publicly available.

7. Actions to Increase Competition: The Government will continue to conduct market research to ascertain if there are changes in the market place that would enable future actions to be competed. Due to the nature of Information Technology and the ever increasing security threats, market research of alternate solutions is an ongoing process.

8. Market Research: In February 2016, the Government's technical experts conducted market research by reviewing similar malware protection full packet capture systems including International Business Machines Security Network Intrusion Prevention System, Cisco IronPort, and PaloAlto WildFire appliances. This market research is an ongoing, continuous process. As a result of that market research, the Government's

technical experts determined that only brand name FireEye appliances are interoperable with the existing EO FireEye architecture and associated infrastructure products, and can provide the required upstream functionality. As described above in section five, no other vendor has the ability to provide the required brand name FireEye appliances, software licenses, and warranty and maintenance support. In August 2016, additional market research was conducted utilizing the NASA SEWP V Market Research Tool, which identified multiple authorized resellers of brand name FireEye hardware, software, and warranty and maintenance support. Therefore, VA anticipates limited competition for this action.

9. Other Facts: None.